(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 091 285 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
11.04.2001 Bulletin 2001/15

(51) Int. Cl.[7]: **G06F 3/12**

(21) Application number: **00308734.3**

(22) Date of filing: **04.10.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **04.10.1999 US 411070**

(71) Applicant:
CANON KABUSHIKI KAISHA
Tokyo (JP)

(72) Inventors:
- **Slick, Royce E.**
  Irvine, California 92612 (US)
- **Mazzagatte, Graig**
  Irvine, California 92612 (US)
- **Iwamoto, Neil Y.**
  Irvine, California 92612 (US)

(74) Representative:
Beresford, Keith Denis Lewis et al
BERESFORD & Co.
High Holborn
2-5 Warwick Court
London WC1R 5DJ (GB)

(54) Targeted secure printing

(57) Secure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient. The data is encrypted using a first key. The first key is then encrypted using a second key and a third key. The second key is a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device. The third key is a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image. The encrypted data and the twice-encrypted first key are transmitted to the intended image output device. The twice-encrypted first key is then decrypted by using the private keys of the second and first key pairs, respectively, which are primarily in the sole possession of the intended recipient device and the intended image output device, respectively. The data is then decrypted and printed at an image output device.

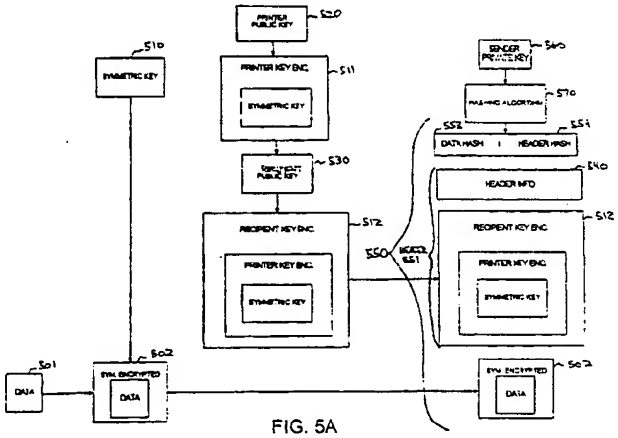

FIG. 5A

EP 1 091 285 A2

EPNSDOCID: <EP 1091285A2 I >

data for generating an image can be transmitted to an image output device, whereby the image is only capable of being printed by the intended image output device in the presence of an intended recipient.

[0014] In another aspect, the invention concerns generation of an image from data transmitted to an intended image output device, such as a printer or a facsimile machine, or such a device itself. The data can be used to generate the image only at the intended image output device in the presence of an intended recipient. Encrypted data and a twice-encrypted first key are received by the device. The encrypted first key is twice decrypted using a second key and a third key, respectively. The second key is a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient. The third key is a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device. After the encrypted first key is twice decrypted, the encrypted data is decrypted using the decrypted first key, and an image is generated by the intended image output device from the decrypted data.

[0015] Preferably, the decryption of the first key using the second and third keys is performed using an asymmetric decryption algorithm. Decryption of the encrypted data using the decrypted first key is preferably performed using a symmetric decryption algorithm.

[0016] Depending upon the order of encryption of the first key, decryption of the first key using the second key can occur before decryption of the first key using the third key. Alternatively, decryption of the first key using the third key can occur before decryption of the first key using the second key.

[0017] In the preferred embodiment, the second key is contained in a smart-card which is in the possession of the intended recipient. Thus, the second key is primarily accessible only with permission by the intended recipient. Likewise, the third key is preferably contained in a smart-chip which is maintained internally in the intended image output device, thereby being shielded from access by devices other than the intended image output device.

[0018] Preferably, the device also receives a header containing information related to the identities of the sender and the recipient. Also, in the preferred embodiment, the receiving step further includes receipt of a signed header hash and a signed data hash. The authenticity of the signed header hash and of the signed data hash preferably are verified using a fourth key which is the public key of a third public key/private key pair; the private key of the third public key/private key pair being primarily maintained in the sole possession of the person who initiated the transmission of the data for receipt by the device. If the signed header hash or the signed data hash fail verification of authenticity, the encrypted data is preferably discarded. Otherwise, the integrity of the signed header hash and the signed data hash are verified by application of a cryptographic hashing algorithm to the header and the encrypted data. If the signed header hash or the signed data hash fail the verification of integrity, the encrypted data is preferably discarded.

[0019] By virtue of the foregoing arrangements, data sent to an image output device is used to generate an image only if the data is intended for that image output device, and only if an intended recipient is present to supply a needed private key.

[0020] Another aspect of the invention concerns secure transmission of data to an intended image output device, wherein the data can be used to generate an image only at the intended image output device in the presence of an intended recipient. In this aspect, the data is encrypted twice using a first key and a second key, the first key being the public key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the second key being the public key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image. The twice-encrypted data is then transmitted to the intended image output device.

[0021] By virtue of the foregoing arrangements, data for generating an image can be transmitted to an image output device, whereby the image is only capable of being printed by the intended image output device in the presence of an intended recipient.

[0022] In another aspect, the invention is directed to generation of an image from twice-encrypted data transmitted to an intended image output device, wherein the twice-encrypted data can be used to generate the image only at the intended image output device in the presence of an intended recipient. In this aspect, twice-encrypted data is received and then twice decrypted by using a first key and a second key. The first key is the private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image. The second key is a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device. An image is then generated from the decrypted data.

[0023] By virtue of the foregoing arrangements, data sent to an image output device is used to generate an image only if the data is intended for that image output device, and only if an intended recipient is present to supply a needed private key.

[0024] In yet another aspect of the invention, a method is provided for secure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient. The

EPODOC: EP

of decryption and printing of a secure print job according to the present invention.

[0030] The present invention is generally directed to the secure printing of image data such that the image data can only be printed on an intended output image device in the presence of an intended recipient. The present invention therefore provides a manner by which a document can be securely transmitted from a computer to a remote image output device in a networked environment. The document is maintained in a secure fashion until the intended recipient is present at the intended image output device, whereupon the intended image output device prints the image.

[0031] Figure 1 provides an overall system view of a networked computing environment in which an embodiment of the present invention may be implemented. As shown in Figure 1, the networked computing environment comprises a network which is connected to desktop computer 10, laptop computer 20, server 40, digital copier 30 and printer 50. Network 100 is preferably an Ethernet network medium consisting of a bus-type physical architecture, although the invention can be utilized over other types of networks, including the Internet.

[0032] Desktop computer 10 is preferably an IBM PC-compatible computer having a windowing environment such as Microsoft Windows 95, Windows 98 or Windows NT. As is typical with IBM PC-compatible computers, desktop computer 10 preferably has a display, keyboard, mouse, floppy drive and/or other type of storage medium (not shown). Also attached to desktop computer 10 is smart-card interface device 15 for interfacing with a smart-card of a computer user, such as smart-card 16. Smart-card 16 therefore provides a mechanism whereby a computer user can authenticate the user's identity to desktop computer 10. In addition, smart-card 16 contains a private key of a private/public key pair which is specific to a computer user and which is used in the present invention for the secure printing of image data as discussed more fully below.

[0033] Laptop computer 20 is also an IBM PC-compatible computer having a windowing environment such as Microsoft Windows 95, Windows 98 or Windows NT. Like desktop computer 10, laptop computer 20 also has a display, keyboard, mouse and floppy drive or other storage means (not shown). In addition, laptop computer 20 also has a smart-card interface device 25 attached to it for interfacing to the smart-card of a computer user such as smart-card 26. Also attached to network 100 is digital copier 30, which is capable of receiving image data over network 100 for printing. Digital copier 30 also has attached smart-card interface device 35 for interfacing with the smart-card of a print job recipient, such as smart-card 36. In addition, server 40 is also connected to network 100. Server 40 preferably comprises an IBM PC-compatible computer having an operating system such as DOS, Microsoft Windows 95, Windows 98 or Windows NT, UNIX or other operating system. Server 40 has a storage device 41 which is preferably a large fixed disk for storing numerous files. Server 40 can therefore be utilized by other devices on network 100 as a file server and may also act as a gateway for other devices on network 100 to another network such as the Internet.

[0034] Printer 50 is also connected to network 100 and is preferably a laser or bubble-jet printer which is capable of operating as both a printer and a facsimile device. Printer 50 has a storage device 51 which is preferably a large fixed disk, and also has an embedded smart-chip 57 which contains a private key of a private/public key pair corresponding to printer 50 for use in encryption and/or decryption of data received by printer 50. In addition, printer 50 is connected to smart-card interface device 55 which is capable of interfacing with a smart-card of a print job recipient, such as smart-card 56. In this manner, the printing of a print job for a particular intended recipient may be controlled through the use of smart-card interface device 55 and smart-card 56, in combination with smart-chip 57 in printer 50.

[0035] Figure 2 is a block diagram showing an overview of the internal architecture of desktop computer 10. In Figure 2, desktop computer 10 is seen to include central processing unit (CPU) 210 such as a programmable microprocessor which is interfaced to computer bus 200. Also coupled to computer bus 200 are keyboard interface 220 for interfacing to a keyboard, mouse interface 230 for interfacing to a pointing device, floppy disk interface 240 for interfacing to a floppy disk, display interface 250 for interfacing to a display, network interface 260 for interfacing to network 100, and smart-card interface 265 for interfacing to smart-card interface device 15.

[0036] Random access memory ("RAM") 270 interfaces to computer bus 200 to provide central processing unit ("CPU") 210 with access to memory storage, thereby acting as the main run-time memory for CPU 210. In particular, when executing stored program instruction sequences, CPU 210 loads those instruction sequences from fixed disk 280 (or other memory media) into random access memory ("RAM") 270 and executes those stored program instruction sequences out of RAM 270. It should also be noted that standard-disk swapping techniques available under windowing operating systems allow segments of memory to be swapped to and from RAM 270 and fixed disk 280. Read-only memory ("ROM") 290 stores invariant instruction sequences, such as start-up instruction sequences for CPU 210 or basic input/output operation system ("BIOS") sequences for the operation of peripheral devices attached to computer 10.

[0037] Fixed disk 280 is one example of a computer-readable medium that stores program instruction sequences executable by central processing unit ("CPU") 210 so as to constitute operating system 281, printer driver 282, smart-card interface driver 283, other

BNSDOCID <EP 1091285A2_I_>

operating system 411, network interface driver 412, encryption/decryption logic 413, e-mail program 414, queue 415, and other files 416. As mentioned above, operating system 411 can be an operating system such as DOS, Windows 95, Windows 98, Windows NT, UNIX, or other such operating system. Network interface driver 412 is utilized to drive network interface 460 for interfacing server 40 to network 100. Encryption/decryption logic 413 allows server 40 to receive encrypted data and to either maintain such data in queue 415 or to send such data to an image output device such as printer 50 for printing. E-mail program 414 is a typical e-mail program and enables server 40 to receive and/or send e-mail messages over network 100. Queue 415 is utilized to store numerous print jobs for output on one or more image output devices, such as printer 50. Lastly, other files 416 contains other files or programs necessary to operate server 40 and/or to provide additional functionality to server 40.

[0045] Figure 5A is a view for explaining the encryption process of the present invention which enables a computer user of a computer on network 100, such as desktop computer 10, to send data related to a print job for printing only on an intended image output device when an intended recipient is present. For instance, a computer user located at desktop computer 10 may wish to prepare a document using word processing program 285 for printing only on printer 50 at a later time when an intended recipient is physically present at printer 50. Most importantly, the computer user at desktop computer 10 wishes to protect the print job data from being accessed or viewed by any device other than printer 50 or by any person other than the intended recipient. Therefore, the present invention encrypts the image data so that it cannot be accessed by any other computer user or device on network 100 and so that it will remain encrypted up until the time the intended recipient is physically present at the intended printer. In this manner, even if the encrypted data is accessed at any point prior to the printing on the intended printer 50, the data will only appear to be a pile of unintelligible bits.

[0046] Specifically, as seen in Figure 5A, the encryption process starts with image data 501 which is preferably created by a computer user at desktop computer 10 using a program such as word processing program 285. When the computer user is ready to send a print job corresponding to data 501 to an intended printer, such as printer 50, for receipt by an intended recipient, the user preferably presses a button provided in word processing program 285 to indicate that the document is to be printed in a secure fashion. In the preferred mode, printer driver 282 handles the encryption process for encrypting data 501 before it is sent over network 100 to printer 50. Preferably, printer driver 282 generates a randomly-generated symmetric key for use with a symmetric encryption algorithm. Data 501 is then encrypted by applying the symmetric encryption algorithm using the randomly-generated symmetric key 510, thereby creating symmetrically encrypted data 502. In this manner, symmetrically encrypted data 502 can only be decrypted by a device having a similar symmetric encryption algorithm and a copy of symmetric key 510. Therefore, symmetric key 510 and symmetrically encrypted data 502 must be passed to printer 50 in order for the data to eventually be decrypted and printed out for the intended recipient. In order to maintain security until such time as data 501 is printed on printer 50, symmetric key 510 is also encrypted with two public keys which correspond to the intended printer and the intended recipient. Each public key is from a public key/private key pair which is used in an asymmetric encryption algorithm. In this manner, only the combination of private keys of the intended recipient and the intended printer will allow symmetric key 510 to be decrypted such that symmetrically encrypted data 502 can be decrypted for printing.

[0047] Therefore, as seen in Figure 5A, printer public key 520 corresponding to printer 50 is obtained from a public key infrastructure which is provided on a server on network 100, from a third-party key service via network 100, or from another suitable source such as a local key storage file. Printer public key 520 is then utilized in conjunction with an asymmetric encryption algorithm to encrypt symmetric key 510, thereby creating printer-key-encrypted symmetric key 511. In this manner, symmetric key 510 cannot be accessed without the corresponding private key of the public/private key pair corresponding to printer 50. As discussed above, the private key for printer 50 is preferably maintained in smart-chip 57 which is embedded within printer 50 so as to prevent exposure of the private key to any other person or device. In this manner, printer key encrypted symmetric key 511 can only be decrypted by the intended image output device, in this case printer 50.

[0048] Although the above encryption of symmetric key 510 ensures that only the intended printer can print the print job, it does not ensure that only the intended recipient will receive the print job for viewing. Therefore, it is also preferable to further encrypt symmetric key 510 with a public key corresponding to the intended recipient. As shown in Figure 5A, recipient public key 530 is also obtained from a public key infrastructure, or other suitable source. The printer-key-encrypted symmetric key 511 is then encrypted again using recipient public key 530 in conjunction with an asymmetric encryption algorithm to create twice-encrypted symmetric key 512. Twice-encrypted symmetric key 512 is shown to be encrypted at a first layer with printer public key 520 and at a second layer with recipient public key 530, thereby preventing access to symmetric key 510 unless the specific combination of private keys of the intended recipient and intended printer is provided.

[0049] As further shown in Figure 5A, a header 540 is provided to contain twice-encrypted symmetric key 512 and also to contain information related to the print job such as the sender's identity, the intended recipi-

authenticated using sender public key 561 to verify that the sender was indeed the creator of print job 550. If the authentication fails, the print job is preferably discarded.

[0056] Next, print job 550 is stored in queue 356 of printer 50 or, in the alternative, is stored in queue 415 of server 40 for subsequent access by printer 50. Once the intended recipient is physically present at printer 50, recipient private key 531 is obtained through the recipient's smart-card, such as smart-card 56, which is inserted into smart-card interface device 55. For security reasons, recipient private key 531 is maintained solely on smart-card 56 and cannot be read by printer 50. Therefore, twice-encrypted symmetric key 512 is passed from printer 50 to smart-card 56 via smart-card interface device 55 where it is partially decrypted using recipient private key 531. Thereafter, partially-decrypted symmetric key 511 is returned from smart-card 56 to printer 50, wherein it is completely decrypted within smart-chip 57 of printer 50. This results in a "clear text" form of symmetric key 510.

[0057] Symmetric key 510 is then utilized to decrypt symmetrically-encrypted data 502 in order to obtain a clear text form of data 501. An image is then printed on printer 50 based upon decrypted data 501. In this manner it can be seen that the present invention provides the ability to transmit a document or image to an intended printer for printing only in the presence of an intended recipient. Until the intended recipient's presence is verified at the location of the intended printer, the print job is maintained in an encrypted form and cannot reasonably be decrypted by any other person or device that may have intercepted the encrypted data.

[0058] Figure 5D is a view for explaining the decryption and printing of twice-encrypted print data 583 which was encrypted pursuant to the alternative of Figure 5B. First, twice-encrypted data 583 is passed to smart-card 56 of the intended recipient via smart-card interface 55, whereupon twice-encrypted data 583 is partially decrypted by using recipient private key 531 which is located in smart-card 56. Smart-card 56 thereupon returns the now partially-decrypted data 582 back to the control of printer 50. Next, partially-decrypted data 582 is passed to smart-chip 57 of printer 50 where partially-encrypted data 582 is completely decrypted using printer private key 521 contained in smart-chip 57 in printer 50. The decrypted, "clear" data 581 is now returned from smart-chip 57 to printer 50 for printing.

[0059] Although the encryption/decryption described in Figures 5B and 5D provide secure printing to an intended printer for an intended recipient, it can be seen that substantially greater resources may be required by smart-chip 57 and smart-card 56 to process twice-encrypted data in comparison to the resources required to process a twice-encrypted symmetric key as depicted in Figures 5A and 5C. Other collateral features depicted in Figure 5B, such as authentication and integrity verification, may also be incorporated in the decryption process of Figure 5D.

[0060] The hashing process depicted in Figure 5A provides signed data hash 553 which is a type of checksum that allows the receiving device, such as printer 50, to verify the integrity of the symmetrically encrypted data 502. Figure 6 shows a view for explaining one method of generating and formatting a signed hash for the data. In Figure 6, print data 601, which corresponds to the image to be securely printed, is in an unencrypted, "plaintext" format. A hashing algorithm, which is preferably a one-way hash function, is then applied to print data 601 to create data hash 610 which is essentially a message digest. Data hash 610 is then digitally signed using the private key of the sender, such as sender private key 560 of Figure 5A. Signed hash 611 may then be optionally encrypted. In either case, signed hash 611 is copied to signed hash 612 which is part of data block 600 for transmission to the intended printer where it is used for authentication and integrity verification purposes.

[0061] Figure 7A is a view for explaining the structure of the header according to a preferred embodiment of the invention. Specifically, recipient ID 701, sender ID 702 and symmetric key 703 are initially provided in a clear, plaintext format for inclusion in header 700 as depicted in Figure 7A. A hashing algorithm is then collectively performed on recipient ID 701, sender ID 702 and symmetric key 703 to create hash 720. Hash 720 is then signed with the private key of the sender, such as sender private key 560 as depicted in Figure 5A, to create signed hash 721. Signed hash 721 may then be optionally encrypted. In either case, signed hash 721 is then copied to signed hash 722 for inclusion in header 700.

[0062] Recipient ID 701 is left in a clear, plaintext format, copied to recipient ID 711 and included in header 700. In the alternative, recipient ID 701 may be encrypted with the public key of the intended printer for anonymity of the intended recipient's identification, copied to recipient ID 711 and included in header 700. In either case, the intended printer can extract and read recipient ID 711 upon receipt of the header, thereby allowing the intended printer to queue the print job corresponding to the intended recipient. Sender ID 702 may be encrypted with the public key of the intended printer before inclusion in header 700, but such encryption is not necessary. Either way, sender ID 702 is copied to sender ID 712 and included in header 700. Symmetric key 703 is preferably twice-encrypted as shown in Figure 5A and then provided in twice-encrypted, symmetric key 713 and included in header 700.

[0063] An alternative structure for the header is shown in Figure 7B whereby the header is structured so that it can be transmitted to the intended printer separately from the encrypted data. Specifically, recipient ID 751, sender ID 752, symmetric key 753 and a uniform resource locator (URL) 754 are initially provided in a clear, plaintext format for inclusion in header 750 as

BNSDOCID <EP 1091285A2>

may also include a URL which points to the location of the encrypted data which corresponds to the header in the case where the header is to be sent separately from the encrypted data. In step S806, a hashing algorithm is then applied to the header to form a header hash and to the encrypted data to form a data hash. The header hash and data hash are then digitally signed with the private key of the sender in step S807. The header hash and data hash may also be optionally encrypted for additional security. Preferably, the private key of the sender is obtained from a smart-card which is kept in the possession of the sender. In the alternative, a token, flashrom or other means of storage can be used to securely store the private key of the sender.

[0070] Next, it is determined in step S808 whether the header is to be sent to the intended printer separate from the corresponding encrypted data. If the header is to be sent separately, control passes to step S809 in which the print job, comprising the header and the header hash, is sent over the network to the intended printer without the corresponding encrypted data. Preferably, the intended printer has an E-mail program and the print job containing the header and header hash is sent to the printer by means of E-mail, although the print job may be separately sent to the intended printer by other means, such as via one or more other network protocols. In the preferred mode, the header contains a URL which corresponds to the location in memory of the encrypted data and data hash. This location can reside on a disk of a computer or server which is accessible by the intended printer via the network. The corresponding encrypted data and data hash are then subsequently sent to the intended printer by the server or computer on which the encrypted data and data hash are stored in step S810, either automatically or at the request of the intended printer by reference to the URL which was provided to the intended printer in the earlier received header. Control then passes to the end (step S812).

[0071] If, however, it is determined in step S808 that the header is not to be sent separately from the corresponding encrypted data to the intended printer, control is passed to step S811 in which a print job comprising the header, header hash, encrypted data, and data hash are transmitted over the network to the intended printer. Control then passes to the end in step S812. In this embodiment, the intended printer receives the encrypted data along with the header which contains the twice-encrypted symmetric key for decryption of the encrypted data. In addition, the header hash and data hash are received by the intended printer for verification of the authenticity and integrity of the header and encrypted data.

[0072] Figure 9 is a flowchart for explaining the decryption and printing of a secure print job according to a preferred embodiment of the present invention. First, the intended printer receives a secure print job in step S901. As discussed above with respect to Figure 8, the print job may only comprise the header and header hash as in the case where the header and header hash are received by the intended printer separately by E-mail. Otherwise, the print job comprises the encrypted data and data hash along with the header and header hash and is received by the intended printer by normal means over the network.

[0073] Next, the public key of the sender is obtained from a public key infrastructure, from another suitable source, or from a copy of the sender's digital certificate provided in the header for use in the subsequent authentication and verification of integrity of the secure print job (step S902). In step S903 the sender's public key is used to check the authenticity of the digital signature of the header hash of the secure print job. If the header hash is not authentic, control passes to step S904 in which a notice is preferably sent to the sender to warn the sender that a non-authenticated print job has been detected. Next, in step S905 the print job is discarded. Flow then passes to the end in step S919. If, however, the header hash is determined to be authentic in step S903, flow passes to step S906 in which the integrity of the header is verified against the header hash.

[0074] In step S906 a hashing algorithm is used to compare the header to the signed data hash to verify that the header was received intact and was not tampered with, therefore indicating that the header is of reliable integrity. If the integrity of the header is in question, control passes to step S905 in which the print job is discarded. Control then passes to the end in step S919. If, however, the header is of reliable integrity, control passes to step S907 in which header information, such as the identity of the intended recipient, is extracted from the header whereupon the print job is placed in a print queue for subsequent printing. Preferably, the print job is sent from the printer to a local server on the network where it is stored in a print queue according to the identification of the intended recipient until subsequently retrieval by the intended printer. In the alternative, the print queue may be maintained in a large memory device within the intended printer itself.

[0075] In step S908, the intended recipient arrives at the location of the intended printer and inserts a smart-card belonging to the intended recipient into a smart-card interface device which is connected to the intended printer. Preferably, the smart-card contains a unique private key and also contains authenticating identification information corresponding to the intended recipient. The printer, via the smart-card interface device, obtains the authenticating identification information of the intended recipient from the smart-card and determined whether the identification of the intended recipient is authentic (step S909). If the identification information is not authentic, control passes to the end in step S919. If the identification information is authentic, the print queue, which is located in either the printer itself or in a local server, is queried, preferably by reference to the identification of the intended recipient, to

image output device in the presence of an intended recipient, the method comprising:

an encrypting step of twice encrypting the data using a first key and a second key, the first key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the second key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; and

a transmitting step of transmitting the twice-encrypted data to the intended image output device.

2. A method for secure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient, the method comprising:

a first encrypting step of encrypting the data using a first key;

a second encrypting step of twice encrypting the first key using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; and

a transmitting step of transmitting the encrypted data and the twice-encrypted first key to the intended image output device.

3. A method according to Claim 2, wherein the first key is randomly generated.

4. A method according to Claim 2, wherein the first encrypting step utilizes a symmetric encryption algorithm.

5. A method according to Claim 2, wherein the second encrypting step utilizes an asymmetric encryption algorithm.

6. A method according to Claim 2, wherein the second encrypting step encrypts the first key using the second key before encrypting the first key using the third key.

7. A method according to Claim 2, wherein the second encrypting step encrypts the first key using the third key before encrypting the first key using the second key.

8. A method according to Claim 2, wherein, in the transmitting step, the twice-encrypted first key is contained in a header which also contains information related to the identity of a device initiating the secure transmission.

9. A method according to Claim 2, wherein, in the transmitting step, the twice-encrypted first key is contained in a header which also contains information related to the identity of a person initiating the secure transmission.

10. A method according to Claim 9, further comprising:

a hashing step of processing the header and the encrypted data with a hashing algorithm, resulting in a header hash and a data hash; and

a signing step of digitally signing the header hash and the data hash with a private key of a third private key/public key pair, the private key of the third private key/public key pair being primarily maintained in the sole possession of the person initiating the secure transmission,

wherein the transmitting step further transmits the signed header hash and the signed data hash.

11. A method according to Claim 2, wherein the intended image output device is a printer.

12. A method according to Claim 2, wherein the intended image output device is a facsimile machine.

13. A method for secure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient, the method comprising:

a first encrypting step of encrypting the data using a first key;

a second encrypting step of twice encrypting the first key using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image;

signed header, if the signed header hash or the signed data hash fail the verification of authenticity and integrity.

27. A method according to Claim 17, wherein the intended image output device is a printer.

28. A method according to Claim 17, wherein the intended image output device is a facsimile machine.

29. A method for generating an image from data transmitted to an intended image output device, wherein the data can be used to generate the image at the intended image output device in the presence of an intended recipient, the method comprising:

a receiving step of receiving a header containing a twice-encrypted first key;
a sending step of sending a request for encrypted data corresponding to the header;
a receiving step of receiving encrypted data corresponding to the header;
a first decrypting step of twice decrypting the twice-encrypted first key using a second key and a third key, the second key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device;
a second decrypting step of decrypting the encrypted data using the decrypted first key; and
an image generating step of generating an image from the decrypted data.

30. A method according to Claim 29, wherein the header is received in the receiving step by e-mail.

31. A method according to Claim 29, wherein the header also contains a reference to a location of the encrypted data, and wherein the request for encrypted data contains the reference to the location of the encrypted data.

32. An apparatus for secure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output device for receipt by an intended recipient, the apparatus comprising:

a memory including a region for storing executable process steps and data for the image; and
a processor for executing the executable process steps;
wherein the executable process steps include (a) an encrypting step of twice encrypting the data using a first key and a second key, the first key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the second key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; and (b) a transmitting step of transmitting the twice-encrypted data to the intended image output device.

33. An apparatus for secure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient, the apparatus comprising:

a memory including a region for storing executable process steps and data for the image; and
a processor for executing the executable process steps;
wherein the executable process steps include (a) a first encrypting step of encrypting the data using a first key; (b) a second encrypting step of twice encrypting the first key using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; and (c) a transmitting step of transmitting the encrypted data and the twice-encrypted first key to the intended image output device.

34. An apparatus according to Claim 33, wherein the first key is randomly generated.

35. An apparatus according to Claim 33, wherein the first encrypting step utilizes a symmetric encryption algorithm.

36. An apparatus according to Claim 33, wherein the second encrypting step utilizes an asymmetric encryption algorithm.

37. An apparatus according to Claim 33, wherein the

BNSDOCID: <EP 1091285A2 >

rily in the sole possession of the intended image output device; and (b) an image generating step of generating an image from the decrypted data.

49. An image output device for generating an image from data transmitted to the image output device, wherein the data can be used to generate the image at the image output device in the presence of an intended recipient, the image output device comprising:

a receiver for receiving encrypted data and an twice-encrypted first key;
an image generator for generating an image from image data;
a memory including a region for storing executable process steps and data; and
a processor for executing the executable process steps, wherein the executable process steps include: (a) a first decrypting step of decrypting the twice-encrypted first key using a second key and a third key, the second key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device; (b) a second decrypting step of decrypting the encrypted data using the decrypted first key; and (c) an image generating step of generating an image from the decrypted data using the image generator.

50. An image output device according to Claim 49, wherein the first decrypting step utilizes an asymmetric decryption algorithm.

51. An image output device according to Claim 49, wherein the second decrypting step utilizes a symmetric decryption algorithm.

52. An image output device according to Claim 49, wherein the first decrypting step decrypts the first key using the second key before decrypting the first key using the third key.

53. An image output device according to Claim 49, wherein the first decrypting step decrypts the first key using the third key before decrypting the first key using the second key.

54. An image output device according to Claim 49, wherein the third key is contained within the image output device, whereby the third key is primarily shielded from access by devices other than the image output device.

55. An image output device according to Claim 49, wherein the second key is contained in a smartcard possessed by the intended recipient, whereby the second key is hidden from recipients other than the intended recipient.

56. An image output device according to Claim 49, wherein the receiving step further receives a signed header hash and a signed data hash, the executable process steps further comprising a verifying step of verifying the authenticity and integrity of the signed header hash and of the signed data hash.

57. An image output device according to Claim 56, wherein the executable process steps further comprise the step of discarding the encrypted data rather than outputting an image, if the signed header hash or the signed data hash fail the verification of authenticity and integrity.

58. An image output device to Claim 57, wherein the executable process steps further comprise the step of sending a notice to a sender of the signed header, if the signed header hash or the signed data hash fail the verification of authenticity and integrity.

59. An image output device according to Claim 49, wherein the image output device is a printer.

60. An image output device according to Claim 49, wherein the image output device is a facsimile machine.

61. An image output device for generating an image from data transmitted to the image output device, wherein the data can be used to generate the image at the image output device in the presence of an intended recipient, the image output device comprising:

a receiver for receiving a header containing a twice-encrypted first key;
an image generator for generating an image from image data;
a memory including a region for storing executable process steps and data; and
a processor for executing the executable process steps, wherein the executable process steps include: (a) a sending step of sending a request for encrypted data corresponding to the header; (b) a receiving step of receiving encrypted data corresponding to the header; (c) a first decrypting step of twice decrypting

resulting in a header hash and a data hash; and

a signing step to digitally sign the header hash and the data hash with a private key of a third private key/public key pair, the private key of the third private key/public key pair being primarily maintained in the sole possession of the person initiating the secure transmission,

wherein the transmitting step further transmits the signed header hash and the signed data hash.

74. A computer-readable medium according to Claim 65, wherein the intended image output device is a printer.

75. A computer-readable medium according to Claim 65, wherein the intended image output device is a facsimile machine.

76. A computer-readable medium which stores computer-executable process steps which securely transmit data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient, the computer-executable process steps comprising:

a data generating step to generate data for an image;

a first encrypting step to encrypt the data using a first key;

a second encrypting step to twice encrypt the first key using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image;

a generating step to generate a header containing the twice-encrypted first key;

a first transmitting step to transmit the header to the intended image output device;

a receiving step to receive a request from the intended image output device for the encrypted data; and

a second transmitting step to transmit the encrypted data to the intended image output device.

77. A computer-readable medium according to Claim 76, wherein the first transmitting step transmits the header to the intended image output device by e-mail.

78. A computer-readable medium according to Claim 76, wherein the header which is generated in the generating step also contains a reference to a location of the encrypted data, and wherein the request for encrypted data contains the reference to the location of the encrypted data.

79. A computer-readable medium which stores computer-executable process steps for generating an image from twice-encrypted data transmitted to an intended image output device, wherein the twice-encrypted data can be used to generate the image at the intended image output device in the presence of an intended recipient, the computer-executable process steps comprising:

a receiving step to receive twice-encrypted data;

a decrypting step to twice decrypt the twice-encrypted data using a first key and a second key, the first key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the second key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device; and

an image generating step to generate an image from the decrypted data.

80. A computer-readable medium which stores computer-executable process steps for generating an image from data transmitted to an intended image output device, wherein the data can be used to generate the image at the intended image output device in the presence of an intended recipient, the computer-executable process steps comprising:

a receiving step to receive encrypted data and a twice-encrypted first key;

a first decrypting step to twice decrypt the twice-encrypted first key using a second key and a third key, the second key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device;

a second decrypting step to decrypt the encrypted data using the decrypted first key; and

an image generating step to generate an image

key/public key pair being primarily in the sole possession of the intended image output device, and the second key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; and

transmitting code for transmitting the twice-encrypted data to the intended image output device.

96. A printer driver which securely transmits data to an intended printer, wherein the data can be used to generate an image at the intended printer in the presence of an intended recipient, the printer driver comprising:

data generating code for generating data for an image;

first encrypting code for encrypting the data using a first key;

second encrypting code for twice encrypting the first key using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/pubiic key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; and

transmitting code for transmitting the encrypted data and the twice-encrypted first key to the intended printer.

97. A printer driver according to Claim 96, wherein the first key is randomly generated.

98. A printer driver according to Claim 96, wherein the first encrypting code utilizes a symmetric encryption algorithm.

99. A printer driver according to Claim 96, wherein the second encrypting code utilizes an asymmetric encryption algorithm.

100. A printer driver according to Claim 96, wherein the second encrypting code encrypts the first key using the second key before encrypting the first key using the third key.

101. A printer driver according to Claim 96, wherein the second encrypting code encrypts the first key using the third key before encrypting the first key using the second key.

102. A printer driver according to Claim 96, wherein the twice-encrypted first key is contained in a header which also contains information related to the identity of a person initiating the secure transmission.

103. A printer driver according to Claim 102, wherein the header also contains a signed header hash and a signed data hash, and further comprising verification code for verification of the authenticity and integrity of the signed header hash and of the signed data hash.

104. A printer driver according to Claim 103, further comprising sending code for sending a notice to a sender of the header, if one of the signed header hash and signed data hash fails the verification of authenticity and integrity.

105. A printer driver which securely transmits data to an intended printer, wherein the data can be used to generate an image at the intended printer in the presence of an intended recipient, the printer driver comprising:

data generating code for generating data for an image;

first encrypting code for encrypting the data using a first key;

second encrypting code for twice encrypting the first key using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image;

generating code for generating a header containing the twice-encrypted first key;

first transmitting code for transmitting the header to the intended image output device;

receiving code for receiving a request from the intended image output device for the encrypted data; and

second transmitting code for transmitting the encrypted data to the intended image output device.

106. A printer driver according to Claim 105, wherein the first transmitting code transmits the header to the intended image output device by e-mail.

107. A printer driver according to Claim 105, wherein the header which is generated in the generating code also contains a reference to a location of the encrypted data, and wherein the request for encrypted data contains the reference to the loca-

121. Computer-executable process steps stored on a computer-readable medium, the computer-executable process steps for generating an image from data transmitted to an intended image output device, wherein the data can be used to generate the image at the intended image output device in the presence of an intended recipient, the computer-executable process steps comprising:

receiving code to receive a header containing a twice-encrypted first key;
sending code to send a request for encrypted data corresponding to the header;
receiving code to receive encrypted data corresponding to the header;
first decrypting code to twice decrypt the twice-encrypted first key using a second key and a third key, the second key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device;
second decrypting code to decrypt the encrypted data using the decrypted first key; and
image generating code to generate an image from the decrypted data.

122. Computer-executable process steps according to Claim 119, wherein the header is received by e-mail.

123. Computer-executable process steps according to Claim 119, wherein the header also contains a reference to a location of the encrypted data, and wherein the request for encrypted data contains the reference to the location of the encrypted data.

124. A signal conveying machine readable instructions for causing a processor to perform a method according to any one of Claims 1 to 31 or for causing the processor to act as a computer for use in an apparatus according to any one of Claims 32 to 47 or for causing the processor to act as an image output device according to any one of Claims 48 to 63 or for causing the processor to act as a printer driver according to any one of Claims 95 to 107.

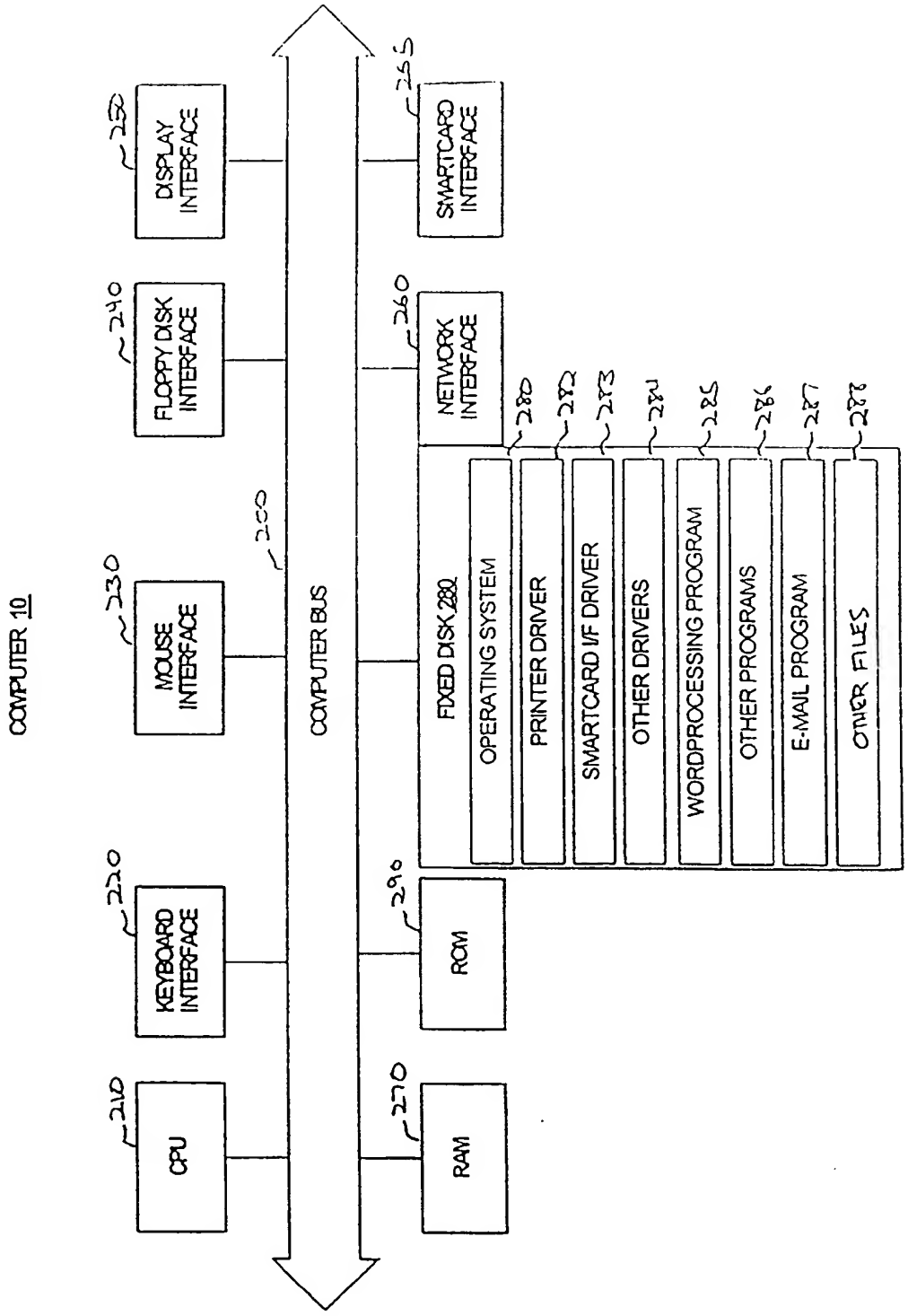
COMPUTER 10
CPU
210
KEYBOARD INTERFACE
220
MOUSE INTERFACE
230
FLOPPY DISK INTERFACE
240
DISPLAY INTERFACE
250
COMPUTER BUS
RAM
270
ROM
290
FIXED DISK 280
OPERATING SYSTEM
PRINTER DRIVER
SMARTCARD I/F DRIVER
OTHER DRIVERS
WORDPROCESSING PROGRAM
OTHER PROGRAMS
E-MAIL PROGRAM
OTHER FILES
NETWORK INTERFACE
260
SMARTCARD INTERFACE
265

FIG. 2

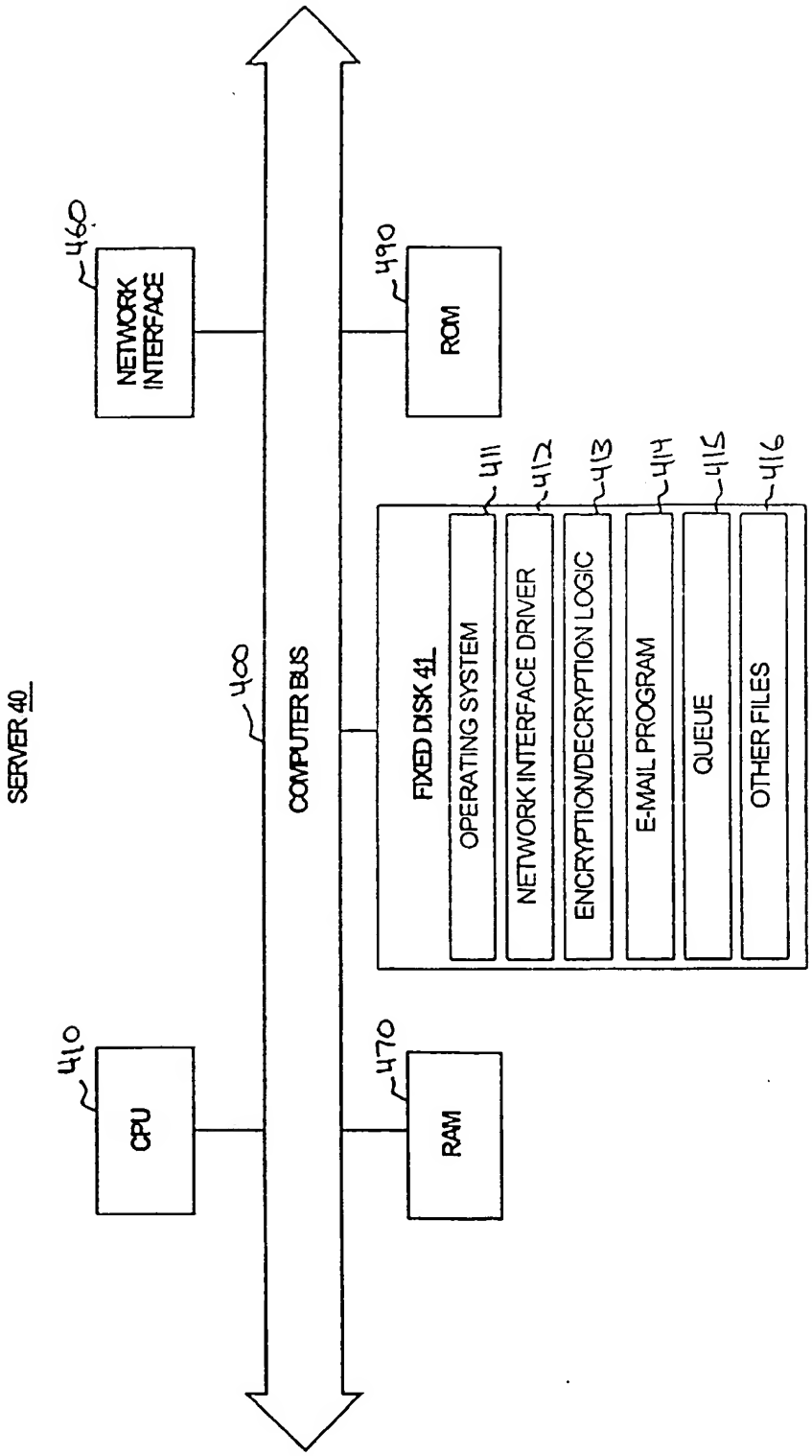
SERVER 40
400
COMPUTER BUS
460
NETWORK INTERFACE
490
ROM
410
CPU
470
RAM
FIXED DISK 41
411
OPERATING SYSTEM
412
NETWORK INTERFACE DRIVER
413
ENCRYPTION/DECRYPTION LOGIC
414
E-MAIL PROGRAM
415
QUEUE
416
OTHER FILES

FIG. 4

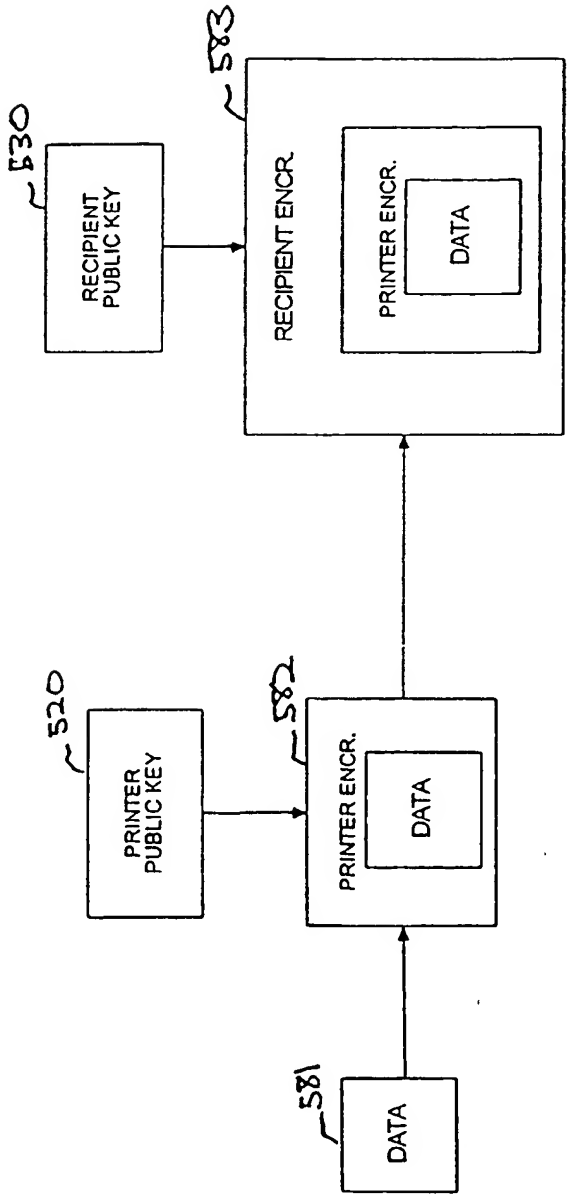
583
530
RECIPIENT PUBLIC KEY
RECIPIENT ENCR.
PRINTER ENCR.
DATA
520
582
PRINTER PUBLIC KEY
PRINTER ENCR.
DATA
581
DATA

FIG. 5B

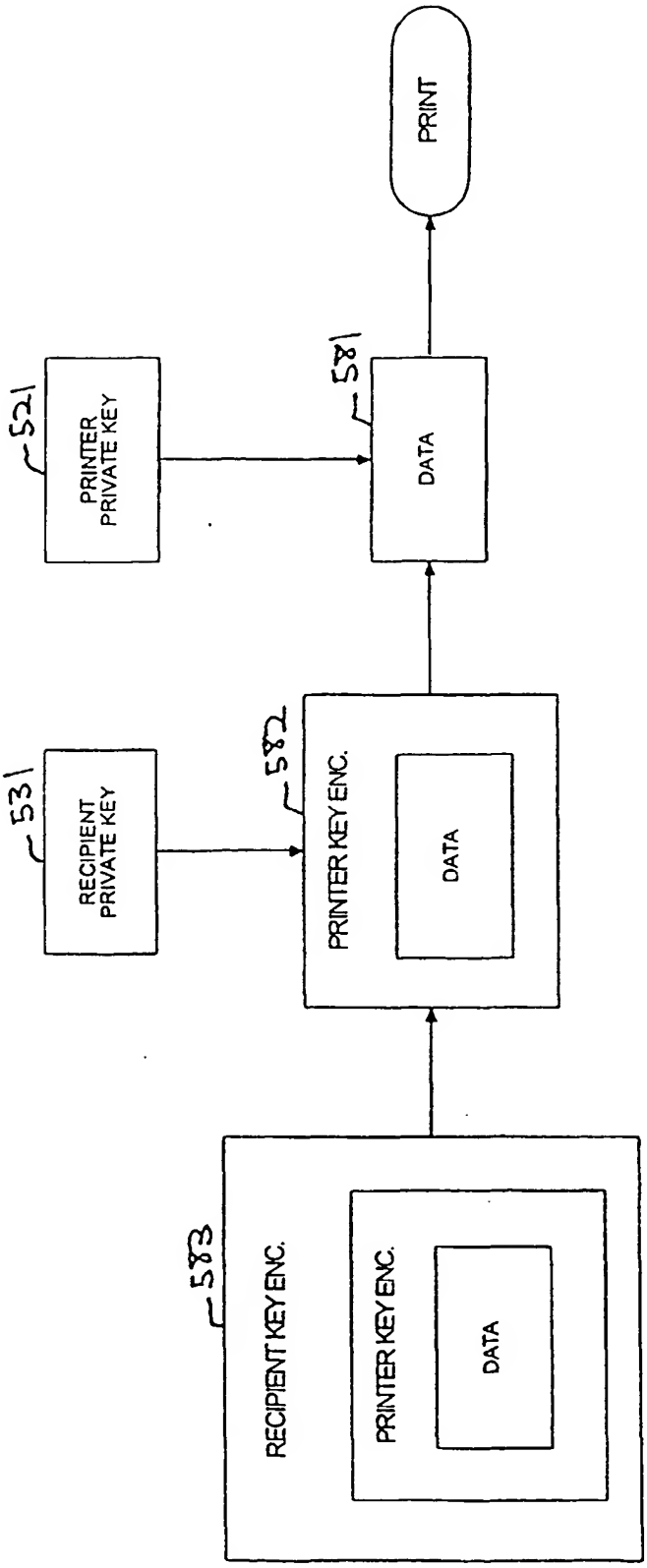
PRINT
581
DATA
521
PRINTER PRIVATE KEY
582
PRINTER KEY ENC.
DATA
531
RECIPIENT PRIVATE KEY
583
RECIPIENT KEY ENC.
PRINTER KEY ENC.
DATA

FIG. 5D

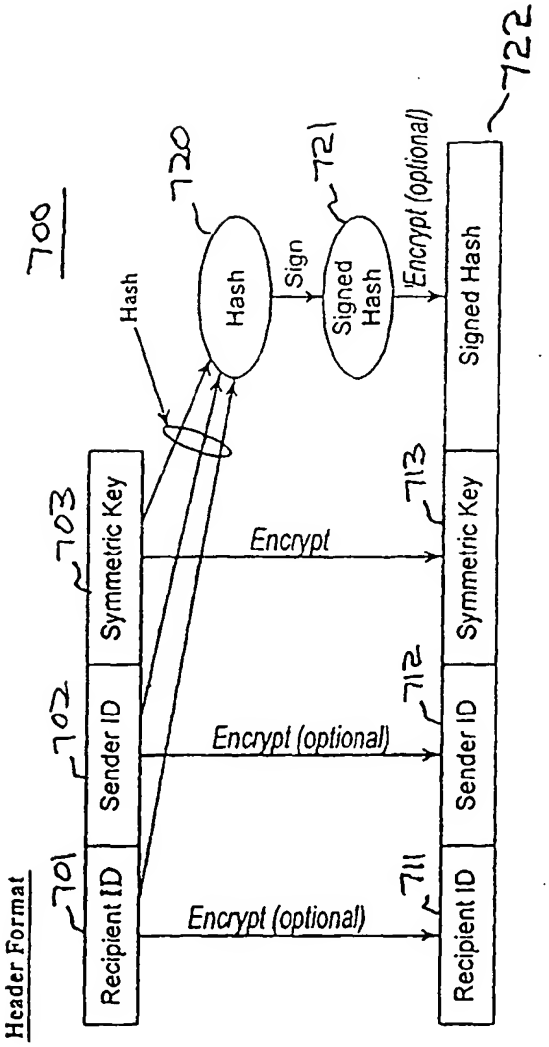
Header Format
Recipient ID
Sender ID
Symmetric Key
Hash
Sign
Signed Hash
Encrypt (optional)
Encrypt
Encrypt (optional)
Encrypt (optional)
Recipient ID
Sender ID
Symmetric Key
Signed Hash
700
701
702
703
720
721
722
711
712
713

FIG. 7A

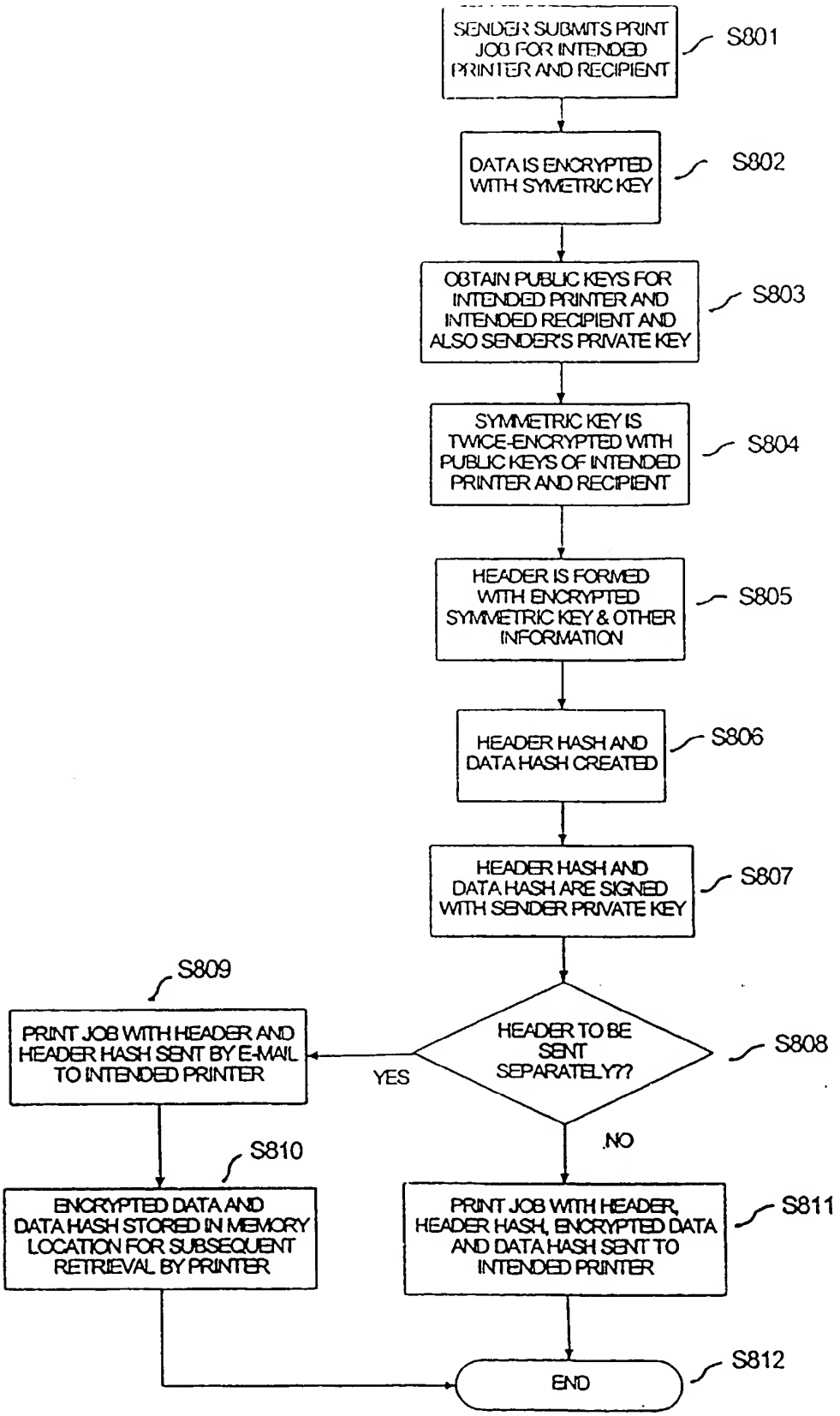
SENDER SUBMITS PRINT JOB FOR INTENDED PRINTER AND RECIPIENT
S801
DATA IS ENCRYPTED WITH SYMETRIC KEY
S802
OBTAIN PUBLIC KEYS FOR INTENDED PRINTER AND INTENDED RECIPIENT AND ALSO SENDER'S PRIVATE KEY
S803
SYMMETRIC KEY IS TWICE-ENCRYPTED WITH PUBLIC KEYS OF INTENDED PRINTER AND RECIPIENT
S804
HEADER IS FORMED WITH ENCRYPTED SYMMETRIC KEY & OTHER INFORMATION
S805
HEADER HASH AND DATA HASH CREATED
S806
HEADER HASH AND DATA HASH ARE SIGNED WITH SENDER PRIVATE KEY
S807
HEADER TO BE SENT SEPARATELY??
S808
YES
NO
S809
PRINT JOB WITH HEADER AND HEADER HASH SENT BY E-MAIL TO INTENDED PRINTER
S810
ENCRYPTED DATA AND DATA HASH STORED IN MEMORY LOCATION FOR SUBSEQUENT RETRIEVAL BY PRINTER
PRINT JOB WITH HEADER, HEADER HASH, ENCRYPTED DATA AND DATA HASH SENT TO INTENDED PRINTER
S811
END
S812

FIG. 8